THE HON. MARY K. DIMKE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON

GLEN MORGAN, individually and on behalf of all others similarly situated, *Plaintiff,* v. TWITTER, INC., *Defendant.*	No. 2:22-cv-00122-MKD FIRST AMENDED CLASS ACTION COMPLAINT JURY DEMAND

I. INTRODUCTION.

1. Plaintiff, individually and on behalf of all others similarly situated, alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and upon information and belief as to all other allegations, based on investigation of counsel. This investigation included, inter alia, a review of public statements and disclosure materials prepared by Defendant; review of Defendant's Securities and Exchange Commission filings; review of pleadings and orders filed in TWITTER, INC. v. ELON R. MUSK, X HOLDINGS I, INC., and X HOLDINGS II, INC., No. 2022-0613-KSJM (Del. Ct. Ch.); review of pleadings and orders filed in UNITED STATES OF AMERICA v.

ARD LAW GROUP PLLC
P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

TWITTER, INC., No. 3:22-cv-3070 (N.D. Cal.); review of publicly available Federal Trade Commission materials related to its investigations of, litigation against, and consent decrees entered into with Defendant; FOIA requests to FTC; review of disclosures made to the United States Congress by Peiter "Mudge" Zatko; media reports; interviews; social media; and other information concerning Defendant. The investigation of the facts pertaining to this case is continuing. Plaintiff believes that substantial evidentiary support exists for the allegations set forth herein, all of which will be capable of proof after a reasonable opportunity for discovery.

2. Privacy and security of personal data is a 21st century civil rights issue that affects everyone who interacts on digital platforms.

3. Behemoth providers of ubiquitous digital platforms make promises of privacy and data security when they solicit users. Too often, those promises are not kept.

4. Many powerful actors who violate individuals' civil rights, including privacy rights and the right to maintain control over personal data disclosed to those platforms, thereafter contest whether any damages resulted from their wrongful conduct.

5. Those powerful companies disregard their promises to users about privacy and data security because of strong financial incentives. Using and trading in private user data can be extraordinarily lucrative for those companies which do so.

ARD LAW GROUP PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

6. This is particularly true for data extracted from and tied to cell phone numbers.

7. As the Washington Supreme Court has recognized, "[t]he ubiquity of cellular devices in modern life has presented and continues to present unique issues of constitutional privacy." *State v. Muhammad*, 194 Wash. 2d 577, 584 (2019).

8. The same companies who routinely trade in users' data tied to phone numbers also routinely contend that, despite the degree to which they profit from refusing to honor the privacy choices exercised by users, there is no comparable, measurable financial harm to those whose rights they violate.

9. Privacy violators also often contend that the harm to an individual is *de minimus*, thereby making it prohibitively expensive for an individual to protect his privacy rights.

10. As with other civil rights violations, legislation has begun to address this issue.

11. As with other civil rights violations, legislatures have established statutory violations, and set a specific amount of statutory damages, together with an award of attorneys' fees and the costs of suit.

12. Washington state has done exactly this, in order to ensure judicial recourse to protect the civil right in privacy of users' phone numbers and other records against improper procurement and use.

13. This suit seeks statutory damages together with attorneys' fees, other costs of litigation, and prejudgment interest, resulting from the acts of Defendant Twitter, Inc. ("Twitter") which engaged in the unauthorized procurement of telephone records of Plaintiff and the Class in violation of RCW 9.26A.140.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

14. Plaintiff is entitled to bring this private action to enforce RCW 9.26A.140 by virtue of that statute and by virtue of RCW 9A.82.010 and 9A.82.100.

II. Jurisdiction and Venue.

15. Subject matter jurisdiction over this matter is proper in Spokane County Superior Court pursuant to RCW 2.08.010 and 7.24.010.

16. Twitter conducts business in Spokane County. Spokane County Superior Court has personal jurisdiction over the parties and venue is proper in Spokane County pursuant to RCW 4.12.020.

III. Parties.

17. Plaintiff Glen Morgan ("Morgan") is a Twitter user with the username @wethegoverned.

18. Plaintiff Morgan was at all times relevant to this Complaint a resident of Washington state.

19. Twitter is a Delaware Corporation with a principal place of business in San Francisco, California.

20. Twitter is a for-profit company.

21. Twitter acts at all times for financial gain.

IV. Facts.

A. The Value of Cellular Telephone Numbers.

22. More than 75% of Washington residents own cell phones.

23. More than 50% of Washington residents own a "smartphone," defined as a cellphone giving the user access to the internet, including apps like Twitter.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

24. Smartphones are used for online shopping, navigation, text messaging and email access.

25. Smartphones save and transmit data, including individualized data concerning matters such as the user's location, shopping habits, and internet searches.

26. This type of smartphone data is tied to and associated with the cell phone number.

27. Data obtained from a user's smartphone have commercial value because of the ability to target advertising likely to be of interest to the user.

28. Data about a smartphone user from a smartphone and associated with the cell phone number, such as internet searches or location, are most valuable when an entity is able to aggregate large quantities of information from many users, and perform analytical functions to predict behavior of the individual smartphone user.

29. Twitter is an entity capable of aggregating large quantities of information about its users.

30. Twitter also has the capacity to analyze user data in order to predict behavior of their users.

31. Twitter has the capacity to give other entities, such as advertisers, access to its user data.

32. Twitter can and does give access to this data based on and exploiting the tie between the data and the user's cell phone number, which a user has provided to Twitter.

33. Giving access to user data has commercial value.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

34. Giving access to user cell phone numbers has commercial value.

35. Smartphone users regard data associated with their cell phone numbers, such as data concerning their internet searches, shopping, and location to be private.

36. Reasonable consumers regard the use of their smartphone data for commercial exploitation without the consumer's consent to be an invasion of privacy.

37. Because sensitive user data is tied to cell phone number, most smartphone users only provide their cell phone number to an entity if they believe that number will only be used for a limited purpose, such as to contact the user.

38. In order to obtain a user's cellphone number, large commercial entities such as UPS or Amazon—and Twitter, as detailed below—explicitly assure the user that the cell phone number will only be used for a limited purpose, such as contacting the user in the event of a problem.

39. Even without explicit assurances from a commercial entity that the cell phone number will only be used for a limited purpose, smartphone users expect that their cell phone number, and data associated with that number, will not be sold or otherwise commercially exploited unless the user consents to such use.

40. In 2011, Twitter and the Federal Trade Commission entered into a Consent Order. The "2011 Consent Order" is attached hereto as Exhibit F and the contests of it are fully incorporated herein.

41. In the 2011 Consent Order, Twitter and the FTC defined "nonpublic consumer information" to mean "nonpublic, individually-identifiable

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

information from or about an individual consumer, including, but not limited to, . . . (c) ***mobile telephone number***; . . .." (Exh. F at 2, emphasis added).

B. Twitter's Assurances Regarding Its Use Of Cell Phone Numbers It Procured.

42. Twitter asks its users to provide a cell phone number in connection with creating a user account.

43. When Twitter asks users for their cell phone numbers, Twitter states that it will use a user's cell phone number for limited purposes, such as to authenticate the identity of the user, to communicate directly with the user, for account recovery purposes, and the like.

44. Twitter also informs users that cell phone numbers are among the data that constitute private user data, sometimes called personally identifiable information.

45. Twitter gives users myriad assurances regarding the safety and security measures it uses to protect private user data, personally identifiable information, and especially cell phone numbers.

46. Twitter promises users that it will be careful with the private information it received from users.

47. Twitter made more detailed and heightened promises regarding its safety and security measures for cell phone numbers than any other category of private user data.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

48. Between May 2007 and November 2009, Twitter told its users "Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information."

49. In 2010 the FTC filed a complaint ("the 2010 FTC Complaint") against Twitter. That Complaint is attached as Exhibit E and fully incorporated herein.

50. In that Complaint, the FTC alleged, inter alia, that "Twitter has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to nonpublic user information and honor the privacy choices exercised by its users in designating certain tweets as nonpublic." Exh. E at 3.

51. In the 2010 FTC Complaint, the FTC alleged that "Twitter also collects certain information about its users that it does not make public. Such information includes . . . ***mobile telephone number*** . . ." Exh. E at 1 ¶ 5 (emphasis added).

52. The 2010 FTC Complaint further alleged that Twitter "represented, expressly or by implication, that it uses reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information."

53. The 2010 FTC Complaint further alleged: "From approximately July 2006 until July 2009, Twitter granted almost all of its employees the ability to exercise administrative control of the Twitter system, including the ability to . . . view a user's nonpublic tweets and other nonpublic user information . . ." Exh. E at 2 ¶ 7.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

54. In 2011 Twitter and the FTC entered into the 2011 Consent Order.

55. The 2011 Consent Order prohibited Twitter from misrepresenting the extent to which Twitter maintained and protected "the security, privacy, confidentiality, or integrity of any nonpublic consumer information . . ." Exh. F at 3.

56. The 2011 Consent Order further prohibited Twitter from misrepresenting "security measures to . . . honor the privacy choices exercised by users." Exh. F at 3.

57. Following the 2011 Consent Order, Twitter continued to assure users that it would safeguard the confidentiality of users' nonpublic information.

58. Twitter's statements were made for the purpose of convincing users to create accounts and associate cell phone numbers with those accounts.

59. Twitter's statements were made to overcome the natural reticence of the reasonable consumer who hesitates to allow a company to obtain his cell phone number because of the risk of a company aggregating the data associated with it to make searching inquiries into the person's private life, all for the purpose of generating profit for the company.

60. To overcome this hesitancy, Twitter made thousands of statements assuring users that it would protect the security and privacy of user data it obtained.

61. Twitter also assured users that, upon receiving a user's request, Twitter would delete the user's account and all associated private data, including any cell phone number provided to Twitter.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

62. Twitter was aware as early as 2006 that users were providing cell numbers based on assurances that Twitter would protect the privacy of user data, including cell numbers.

63. Following the 2011 Consent Order, consumers would be entitled to assume that Twitter was complying with the terms of that Order.

C. The 2019 Twitter Disclosure.

64. On October 8, 2019 Twitter publicly acknowledged that "when [users] provided an email address or phone number for safety or security purposes (for example, two-factor authentication) this data may have inadvertently been used for advertising purposes, specifically in our Tailored Audiences and Partner Audiences advertising system."[1]

65. When Twitter made this disclosure, it had been providing to all users various screens purportedly for account management that purported to give users the ability to control the use to which Twitter put phone numbers it had procured, including specifically whether the user did or did not agree to accept advertising that was targeted to the user based on the user's cell phone number that the user had provided to Twitter.

66. Unbeknownst to any Twitter user, Twitter disregarded the choices exercised by users, as evidenced to Twitter through the account settings selections made on those screens.

[1] *See* https://help.twitter.com/en/information-and-ads#10-08-2019 (last accessed December 9, 2022).

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

67. In doing so, Twitter also disregarded literally tens of thousands of other promises it had made to users regarding the safety and security of cell phone numbers.

68. In doing so, Twitter also violated the 2011 FTC Consent Order, and the promises to users contained in that public agreement.

69. Users who gave cell phone numbers to Twitter had reasonably relied on Twitter's thousands of statements regarding the safety and security of user data, especially including personally identifiable information including cell phone numbers.

70. Twitter's 2019 disclosure revealed that it had not complied with any of its promises to users, that had resulted in users providing cell phone numbers to Twitter.

D. The 2022 Mudge Disclosure.

71. On or about July 6, 2022, Peiter "Mudge" Zatko (hereafter, "Mudge") made two Whistleblower Disclosures to the United States Congress.

72. The United States Sente Judiciary Committee refers to the disclosures as the "Alpha" and "Bravo" disclosures.

73. The Alpha Disclosure is available at https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower, and is attached hereto as Exhibit A. The contents of the Alpha Disclosure are fully incorporated herein.

74. Mudge attached 42 exhibits to the Alpha Disclosure. Those exhibits, other than Exhibits 12, 18, and 29 are available at

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower. The available exhibits are attached hereto as Exhibits A-1 to A-42, the contents of which are incorporated fully herein.[2]

75. The Bravo Disclosure is available at https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower, and is attached hereto as Exhibit B. The contents of the Bravo Disclosure are fully incorporated herein.

76. Mudge attached 6 exhibits to the Bravo Disclosure, available at https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower, and which are attached hereto as Exhibits B-1 to B-6. The contents of Exhibits B-1 to B-6 are incorporated fully herein.

77. Mudge submitted a written copy of his initial testimony, available at https://www.judiciary.senate.gov/download/testimony-zatko-2022-09-13, and attached hereto as Exhibit C, the contents of which is incorporated fully herein.

78. Mudge also responded in writing and under oath to subsequent questions, available at https://www.judiciary.senate.gov/download/responses-to-questions-for-the-record-zatko-2022-09-13, and attached hereto as Exhibit D, the contents of which is incorporated fully herein.

[2] All files and screens from the Judiciary Committee were last accessed on November 30, 2022. The available files list does not include Exhibits 12 and 18; the hyperlink to Exhibit 29 goes to a 404 error page as seen in the attached Exh. A-29.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

79. Mudge testified that he was employed by Twitter as "'Security Lead', a member of the senior executive team responsible for Information Security, Privacy, Physical Security, Information Technology, and 'Twitter Service' (the corporate division responsible for global content moderation enforcement) at Twitter, Inc. from November 16, 2020, until the morning of January 19, 2022." Exh. A at 2.

80. In the disclosures, Mudge testified that during his employment he had "uncovered extreme, egregious deficiencies by Twitter in every area of his mandate including (as described in detail below) user privacy [and] digital and physical security . . ." Exh. A at 2.

81. Mudge testified that "since 2011 and on an ongoing basis" Twitter "engaged in [e]xtensive, repeated, uninterrupted violations of the Federal Trade Commission Act by making false and misleading statements to users and the FTC about, inter alia, the Twitter platform's security, privacy, and integrity." Exh. A at 2-3.

82. Mudge testified that "since 2011 and on an ongoing basis" Twitter "engaged in" "[n]egligence ***and even complicity*** with respect to efforts by foreign governments to ***infiltrate***, control, exploit, ***surveil*** and/or censor the company's platform." Exh. A at 3 (emphasis added).

83. Mudge testified that Twitter made near-constant assurances to users and its regulators regarding its supposed attention to the security and privacy of user data.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

84. Mudge attached to his testimony a document titled "Q4 2021 Privacy & Data Protection Report," attached hereto as Exh. A-15.

85. In that document, he testified to preparations Twitter had made to attempt to come into compliance with the forthcoming demands of the 2022 FTC Consent Decree that Twitter intended do—and eventually did—enter into in order to resolve the violations of the 2011 Consent Order revealed by the 2019 Disclosure detailed above.

86. The document showed that in late 2021, Twitter was attempting to "ensur[e that] Existing Products, Services, and Systems Operate Consistent with Existing Security and Privacy Statements." Exh. A-15 at 3.

87. To do so, a group at Twitter (presumably Mudge's team) had "collected 5 years worth of statements (i.e. >20k statements) regarding privacy promises . . ." Exh. A-15 at 3 (emphasis added).

88. On average, Twitter made at least 4,000 public statements per year assuring users that it would protect their privacy.

89. Mudge also testified that, as of the date of his testimony, he did not know of a single one of Twitter's hundreds of products and services that had been analyzed to determine whether they "operat[ed] consistently with [Twitter's] existing statements" regarding safety and security of user data including cell phone numbers.

90. Between 2011, when the 2011 Consent Order was agreed to, and the time of Mudge's testimony, Twitter never conducted an internal audit of whether it was complying with the promises made in the 2011 Consent Order.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

91. Mudge testified that Twitter had ***never*** complied with its obligations under the 2011 FTC Consent Order.

92. Mudge testified that "The 2011 FTC Consent Order and the 2020 FTC Draft Complaint both identified protection of sensitive user data as crucial problems to be addressed. But in the decade since then, things actually got meaningfully worse, with ***sensitive customer information like*** emails and ***phone numbers improperly used for marketing***, simultaneously while the company negotiated a new settlement with the FTC in 2020 and 2021." Exh. A at 71 (emphasis added).

E. The Falsity of Twitter's Representations Concerning Its Protection of Users' Private Information, Including Cellphone Numbers.

93. The 2011 Consent Order describes Twitter's false representations concerning the security measures it took to insure users' privacy.

94. The 2011 Consent Order found that "Between January and May 2009, intruders exploited the failures . . . to obtain unauthorized administrative control of the Twitter system. Through this administrative control, the intruders were able to: (1) gain unauthorized access to . . . nonpublic user information." Exh. E at 4 ¶ 12.

95. The FTC alleged that Twitter "represented, expressly or by implication . . . that it uses reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information." Exh. E at 5 ¶ 15.

96. The FTC alleged that "In truth and in fact . . . [Twitter] did not use reasonable and appropriate security measures to prevent unauthorized access

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

to nonpublic user information. Therefore, [Twitter's] representation . . was, and is, false or misleading." Exh. E at 5 ¶ 16.

97. The FTC alleged that "[Twitter] has represented, expressly or by implication, that it uses reasonable and appropriate security measures to honor the privacy choices exercised by users. In truth and in fact . . . [Twitter] did not use reasonable and appropriate security measures to honor the privacy choices exercised by users. Therefore, the representation . . . was, and is, false or misleading." *Id.*

98. Twitter consented to the 2011 Consent Order with the FTC.

99. In the 2011 Consent Order, Twitter committed that it would not thereafter "misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, including, but not limited to, misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users." Exh. F at 3.

100. Twitter also agreed that it would, from that date forward, "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information." *Id.*

101. Twitter agreed that the "program [would] contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity." *Id.*

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

102. Twitter agreed that the safeguards would include "the designation of an employee or employees to coordinate and be accountable for the information security program" called for by the Order. *Id.*

103. Twitter agreed that the safeguards would include systems for "the identification of reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information or in unauthorized administrative control of the Twitter system, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, account takeovers, or other systems failures." *Id.*

104. Twitter also committed that it would "deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order." Exh. F at 6.

105. As detailed herein, neither before nor after the 2011 Consent Order did Twitter ever comply with the obligations it had proffered to users prior to the 2011 Consent Order, the violation of which had led to that investigation and Consent Order.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

106. As detailed herein, Twitter did not comply with the obligations it assumed when it entered into the 2011 Consent Order.

F. Twitter's Near-Constant Violations Of Its Representations To Users And Governments.

107. One of the specific violations that the FTC demanded Twitter address in the 2011 Consent Order was that Twitter had allowed a vast percentage of its employees to have almost complete access to any and all data and code at Twitter—including a level of complete control and access referred to as "God Mode" access.

108. Yet Mudge testified that by January 2021 he found "serious access control problems, with far too many staff (about half of Twitter's 10,000 employees, and growing) given access to sensitive live production systems and user data in order to do their jobs, the subject of specific misrepresentations in 2020 by then-Chief Technology Officer Parag Agrawal." Exh. A at 27-28.

109. Mudge testified that Agrawal's statements, made in response to the 2020 hack and for the purpose of reassuring users as to the safety and security of their private data including cell phone numbers, were either outright falsehoods or fundamentally misleading as to the employee access problem—a problem Twitter had committed in the 2011 FTC Consent Order that it would fix.

110. Mudge testified to Congress that the opposite was true: "at the end of 2021, 51 % of the ~ 11 thousand full-time employees had privileged access to Twitter's production systems, a 5% increase from the 46% of total employees

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

in February of 2021 that Mudge had shared in his initial findings delivered to the Board in early 2021." Exh. A at 43.

111. Profligately giving employees access to vast quantities of private user data, including cell phone numbers, wasn't bad enough for Twitter. As Mudge testified, "Twitter did not actively monitor what employees were doing on their computers. Although against policy, it was commonplace for people to install whatever software they wanted on their work systems. Twitter employees were repeatedly found to be ***intentionally installing spyware on their work computers at the request of external organizations***." Exh. A at 26 (emphasis added).

112. Twitter's assurances to users regarding the safety and security of private data, including cell phone numbers, were contradicted by Twitter's conduct that included allowing those employees with "God Mode" access to private data, including cell phone numbers, to also install spyware at the request of external organizations.

113. Twitter also did not delete user data, including cell phone numbers, despite telling users it could and would do so on request.

114. In fact, Mudge testified that Twitter intentionally and knowingly misled the FTC and users regarding its ability to comply with promises to delete user data on request, implying that it could and did delete sensitive, private user data including cell phone numbers, but actually not doing so because it was incapable.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

G. Twitter Violated RCW 9.26A.140(1)(b): Obtaining Telephone Records Through Fraudulent, Deceptive, Or False Means.

115. Twitter obtained a telephone record which pertains to Morgan.

116. Specifically, Twitter obtained Morgan's cell phone number from Morgan.

117. Twitter obtained Morgan's cell phone number on July 30, 2016.

118. Twitter did so after promising Morgan that Twitter would protect the nonpublic information in his account, including his cell phone number, from unwanted disclosure.

119. Twitter did not use reasonable means to protect Morgan's private data, including his cell phone number, from unwanted disclosure.

120. Twitter knew that the means it had been employing to protect user data, including cell phone numbers, from unwanted disclosure were inadequate.

121. Twitter knew that it was not exercising reasonable controls to limit the use of Morgan's cell phone number to the purposes he selected and that Twitter had promised.

122. Twitter knew that its assurances of reasonable protection of cell phone numebrs from unwanted disclosure were false.

123. When Twitter obtained Morgan's cell phone number it did so through the use of deceptive and/ or false means.

124. The deceptive means used to obtain Morgan's telephone number included assurances that Morgan could choose the extent to which his user data, including his cell phone number, could be exploited by Twitter for commercial purposes.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

125. Twitter obtained telephone records which pertain to other Washington persons.

126. Twitter did so with the same deceptive and/ or false means it employed to obtain Morgan's cell phone number.

H. Twitter Violated RCW 9.26A.140(1)(a): Sale of Telephone Records.

127. Twitter obtained the cell phone numbers of Morgan and other Washington residents with the assurance that those numbers would only be used for limited purposes and protected from disclosure.

128. Twitter was able to increase its advertising revenue by offering to advertisers access to user data, including cell phone numbers.

129. Twitter used the user data obtained from users, including cell phone numbers, for financial gain.

130. Specifically, on information and belief, a reasonable opportunity for discovery will reveal that Twitter charges advertisers more for ads that target users based on cell phone numbers.

131. On information and belief, a reasonable opportunity for discovery will show that Twitter also released cell phone numbers to outside entities, including advertisers.

132. For example, Mudge reported that in 2021, Twitter's "CFO complained to Mudge that his request to send a large collection of user emails to an advertiser was being blocked by a few engineers. Mudge explained that the engineers were right to be blocking it, because Twitter did not have any understanding

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

of data-lineage and there was no indication whether Twitter sending this data to a customer would be violating the FTC consent decree." Exh. A at 25.

133. Given Twitter's pervasive lack of concern about its treatment of any private, personally identifying user data, this occurrence reasonably supports the belief that a reasonable opportunity for discovery will also reveal similar instances where Twitter transferred cell phone numbers to advertisers for money despite that it had promised users not to do so.

134. On information and belief, a reasonable opportunity for discovery will reveal that Twitter's advertisers demand assurances that, when they pay additional amounts for targeted advertising, they receive the benefit of the bargain.

135. On information and belief, a reasonable opportunity for discovery will reveal that Twitter's advertisers demand proof that advertising for which they pay additional amounts is, in fact, targeted to users' telephone numbers.

136. On information and belief, a reasonable opportunity for discovery will reveal that Twitter's advertisers who pay additional amounts for targeted advertising to Twitter users thereafter receive information regarding targeted advertising that constitutes "telephone records" of those users under RCW 9.26A.140.

137. If so, Twitter thereby "[i]ntentionally [sold] the telephone record of any resident of this state without the authorization of the customer to whom the record pertains." RCW 9.26A.140.

138. If so, it committed that act of sale for financial gain.

139. Finally, on information and belief, and based on the Mudge Disclosure, Plaintiff believes that a reasonable opportunity for discovery will show that

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

Twitter's disregard of its promises to users regarding the safety and security protection of their private data, including cell phone numbers, as well as its constant public misrepresentations of the same to suers, regulators, and governments, continues today.

I. Civil Remedy.

140. Due to the foregoing conduct, Twitter is "subject to legal action for injunctive relief and either actual damages, including mental pain and suffering, or liquidated damages of five thousand dollars per violation, whichever is greater." RCW 9.26A.140.

141. Each telephone number Twitter procured from a Washington person constitutes a separate violation of RCW 9.26A.140, subject to $5,000 liquidated damages.

142. Morgan has sustained injury to his person, business, or property by Twitter's acts that are part of a pattern of acts included in RCW 9A.82.010(4)(nn).

143. Morgan may therefore file an action for the recovery of damages and the costs of the suit, including reasonable investigative and attorney's fees.

V. Class Allegations.

144. Morgan brings this action as a class action pursuant to Washington Civil Rules 23(a) and 23(b) on behalf of the following Class of persons:

All Washington persons who provided a telephone number to Twitter associated with a Twitter account.

145. Excluded from the Class is any person, firm, trust, corporation, or other entity related to or affiliated with Defendant.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

146. Morgan reserves the right to amend the Class definition if further investigation and/or discovery indicate that the Class definition should be narrowed, expanded, or otherwise modified.

147. Upon information and belief, numerous Washington persons provided telephone numbers to Twitter.

148. According to Don Hoffman, who as of May 18, 2022[3] was a "Senior Software Engineer" at Twitter, "there are at least 10,000 Twitter users who Twitter has reason to believe are in Washington State, and who 'provided a telephone number to Twitter associated with a Twitter account prior to September 17, 2019.'"

149. Upon information and belief, the number of individuals and entities who comprise the Class are so numerous that joinder of all such persons is impracticable and the disposition of their claims in a class action, rather than in individual actions, will benefit both the parties and the courts.

150. Upon information and belief, class members may be identified from records maintained by Defendants, and may be notified of the pendency of this action by mail or electronic mail using the form of notice similar to that customarily used in class actions, including by using Twitter's service.

151. Morgan's claims are typical of the claims of the other members of the Class. All members of the Class have been and/or continue to be similarly affected by Defendant's wrongful conduct as complained of herein. Morgan is unaware

[3] Plaintiff does not know whether Mr. Hoffman is among the Twitter employees who ceased to work for Twitter during the latter half of 2022.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

of any interests that conflict with or are antagonistic to the interests of the Class.

152. Morgan will fairly and adequately protect the Class members' interests and has retained counsel competent and experienced in class actions and complex litigation. Morgan and Morgan's counsel will adequately and vigorously litigate this class action, and Morgan is aware of his duties and responsibilities to the Class.

153. Defendant has acted with respect to the Class in a manner generally applicable to each Class member. Common questions of law and fact exist as to all Class members and predominate over any questions affecting individual Class members. The questions of law and fact common to the Class include, *inter alia*:

a. Whether Defendant obtained telephone records which pertain to residents of this state through deceptive and/ or false means;
b. Whether Defendant intentionally sold the telephone records of residents of this state; and
c. The remedies available to Morgan and the Class.

154. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, as the injury and/or damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation makes it impossible as a practical matter for Class members to individually redress the wrongs done to them. There will be no difficulty in managing this action as a class action.

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

155. Defendant has acted on grounds generally applicable to the entire Class with respect to the matters complained of herein, thereby making appropriate the relief sought herein with respect to the Class as a whole.

VI. Cause Of Action

156. Morgan hereby incorporates by reference the allegations contained in the preceding paragraphs of this Complaint.

157. This sole Count is brought pursuant to RCW 9.26A.140 and RCW 9A.82.100, on behalf of the Class, against Defendant.

158. Defendant obtained telephone records of residents of this state through deceptive and/ or false means.

159. Pursuant to RCW 9.26A.140, Morgan and each member of the Class is entitled to $5,000 in liquidated damages for each such violation.

VII. Prayer For Relief

Wherefore, Morgan and the Class pray for relief and judgment as follows:

A. Declaring that this action is properly maintainable as a class action, and certifying Morgan as the Class representative and Morgan's counsel as Counsel for the Class;

B. Declaring that Defendant engaged in the unauthorized procurement of telephone records under RCW 9.26A.140;

C. Declaring that Defendant engaged in the unauthorized sale of telephone records under RCW 9.26A.140;

Ard Law Group PLLC

P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

D. Awarding Morgan and the members of the Class the remedy of statutory damages of $5,000 for each violation, together with pre- and post-judgment interest;

E. Awarding costs of investigation and litigation, including expert witness costs, and reasonable attorneys' fees, against Defendant;

F. Enjoining Defendant from further violations of RCW 9.26A.140; and

G. Such other and further relief as this Court may deem just and proper.

VIII. Jury Demand

Morgan and the Class hereby demand a trial by jury.

///

///

///

///

///

Ard Law Group PLLC	Albrecht Law PLLC
By: _____	By: _____
Joel B. Ard, WSBA # 40104 P.O. Box 11633 Bainbridge Island, WA 98110 206.701.9243 Joel@Ard.law	David K. DeWolf, WSBA #10875 5105 E 3rd Ave., Suite 101 Spokane Valley, WA 99212 (509) 495-1246 david@albrechtlawfirm.com